07/16/2010

Defense Security Service (DSS) Notice to Cleared Companies

Subject: Potential Disclosure of Contract Information

Early next week, we expect the Washington Post to publish articles and an interactive website that will likely identify government agencies and contractors allegedly conducting Top Secret work. The website is expected to enable users to see the relationships between the federal government and its contractors, describe the type of work the contractors perform, and may identify many government and contractor facility locations.

Publication is expected starting on or about July 19, 2010, with additional articles published thereafter. We anticipate the article series and website will generate follow-on national media interest, as well as media interest in the local cleared companies.

If approached by any media outlets regarding these articles or website, please be mindful of the public release provisions stated in Block 12 of the Contract Security Classification Specification (DD Form 254) issued with each of your contracts that involve access to classified information. Any public release of information regarding classified contracts requires review by and approval of your Government Contracting Activity, except as authorized by Paragraph 5-511 of the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M.

Should your management or public affairs offices be contacted by the media, if appropriate, you may refer media inquiries to Office of the Assistant Secretary of Defense for Public Affairs at 703-697-5131.

We recognize that this information can be put to legitimate use. However, without a doubt, foreign intelligence services, terrorist organizations, and criminal elements will also have interest in this kind of information. It is important that companies continually review their overall security posture to ensure that it meets required standards. We recommend that companies affected by this publication and website assess, and take steps to mitigate, risk to their workforce, facility and operations. These steps should include reinforcement of security and counterintelligence (CI) protections, and a dedicated effort to enhance workforce awareness of threats. This is also a good opportunity to review the contents of your website to ensure that it does not contain information for which you should have received prior release approval. Security and CI events related to the publication of these articles and website should be reported through normal company channels to your Facility Security Officer and DSS Industrial Security Representative.

If you have any questions, requests for specific guidance, and/or want to report any unusual activity, please don't hesitate to have your Facility Security Officer work with the local DSS Industrial Security representative. DSS is committed to working with companies to safeguard classified information.

Kathy Watson
Director